USAWC STRATEGY RESEARCH PROJECT

NATIONAL SECURITY POLICY ON GOVERNMENT SECRECY

by

Alan F. Brown
Defense Leadership and Management Program

CDR Phillip Pattee
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
07-04-2003		xx-xx-2002 to xx-xx-2003

4. TITLE AND SUBTITLE
National Security Policy on Government Secrecy
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Brown, Alan F. ; Author

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
U.S. Army War College
Carlisle Barracks
Carlisle, PA17013-5050

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
			Same as Report (SAR)	29	Rife, Dave RifeD@awc.carlisle.army.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number DSN

ABSTRACT

AUTHOR: Alan F. Brown

TITLE: National Security Policy on Government Secrecy

FORMAT: Strategy Research Project

DATE: 07 April 2003 PAGES: 18 CLASSIFICATION: Unclassified

Protecting certain information in government is vital to the national security and public safety. The American public has the right to know of the activities of its government. How has the balance of secrecy and openness in the national security policy changed over the years? Where is the Federal Government headed with its national security policy on secrecy?

TABLE OF CONTENTS

NATIONAL SECURITY POLICY ON GOVERNMENT SECRECY

> It is the business of a general to be quiet and thus ensure secrecy; upright and just, and thus maintain order. He must be able to mystify his officers and men by false reports and appearances, and thus keep them in total ignorance. By altering his arrangements and changing his plans, he keeps the enemy without definite knowledge. By shifting his camp and taking circuitous routes, he prevents the enemy from anticipating his purpose.
>
> —Sun Tzu, Art of War

Some information in government is vital to the national security and cannot be disclosed publicly. Yet citizens of the United States of America have a constitutional right to know the activities of its government. A critical balance must be maintained between secrecy and openness in government. Such a balance is vital to the efficiency, integrity, timeliness, and effectiveness of the government's information and operations. This balance is also crucial to the people's support of the government.

Understandably, certain information held by the government must be kept secret in the interest of national security and public safety, and must be protected from unauthorized, improper or inadvertent disclosure to adversaries of the United States. The public does not need to be privy to all government information, such as sources of intelligence information whose exposure may jeopardize someone's life or enable an adversary of the nation to attack our homeland. National security is defined as "the national defense or foreign relations of the United States."[1] Information classified as national security information is related to the national defense or foreign relations of the United States and if disclosed to an adversary, could have a damaging effect on the welfare and security of the nation. The act of classification is the process by which information in possession or under control of the government is identified as requiring protection from disclosure, hence the term, "classified information." The nation's policy on government secrecy exists to protect national security. That policy is manifested in a security classification system intended to guard the nation's secrets that protect Americans from harm yet provides for an informed public.

Secrecy, by itself, can infer that certain war plans, weapons capabilities, technology, countermeasures, and related activities exist. Secrecy can serve as an indicator of sensitive or classified research, plans, capabilities, or actions. The absence of certain information in the public domain or gaps in disclosed information may provide an adversary an indication that the United States Government is contemplating sensitive activities or countermeasures.

Extreme secrecy can have a significant detrimental effect on national policy when it precludes an informed public, contributes to inadequate accountability of the government's actions, and allows for ill-informed policymakers. Though some secrecy is important to saving lives, protecting national security, and engaging in sound diplomacy, too much secrecy is expensive, contributes to the public's distrust of government programs and systems, and degrades public service.[2]

More openness relative to the secrecy of information allows for greater understanding by the public of the government's actions. It also helps the government respond to public criticism by informing the public of the reasons for its actions. A more relaxed flow of information contributes to greater scientific discovery, promotes development and application of new technologies, and provides for greater learning through examination of past experiences. Where are we today with regard to secrecy and openness? Do we have a healthy balance or is the government skewed with its secrecy policy? This document examines our history of secrecy and how it has evolved as a national policy. It looks at how a critical balance must be maintained to ensure a strong, positive relationship between the government and the people it serves.

ORIGIN OF SECRECY POLICY

To understand the government's policy today, we look at the history of secrecy. When or where did the concept of secrecy by government begin? Taking actions to keep information secret dates back to the earliest annals of history. The concealment of Greek soldiers in the Trojan Horse was undoubtedly *classified information* until the soldiers suddenly appeared and attacked the ancient city of Troy. As early as 300 BC in *The Art of War*, Sun Tzu wrote "the formation and procedure used by the military should not be divulged beforehand."[3] The initiative of protecting from disclosure information over two millennia ago is still applicable today. It has application to military strategy as well as business information and financial statistics.

In America, members of the First Continental Congress started the process of classifying information for secrecy on September 6, 1774, when they passed the resolution: "Resolved, that the doors be kept shut during the time of business, and that the members consider themselves under the strongest obligations of honor, to keep the proceedings secret, until the majority shall direct them to be made public." This may be the first indication of the government's concern that information under consideration, or *pre-decisional*, might affect the welfare and security of the nation if disclosed prematurely, that is before significant proposals are accepted and decisions are made and publicized.

In 1775, the new nation's Articles of War addressed unauthorized disclosure of information by members of the Continental Army. The first directive issued by the government on secrecy of information occurred in 1869 and pertained to safeguarding information on Army fortifications.[4] This is the earliest indication that the government was concerned for its security, from a national policy standpoint, and took regulatory action to curtail disclosure.

One might believe the idea for the national secrecy policy, which formed the basis of today's modern system for classifying and protecting national security information, came from the military. Actually, physicists working on the development of nuclear weapons originally proposed the policy. In 1939, with World War II impending, Leo Szilard urged Albert Einstein to petition President Roosevelt to issue a government secrecy policy.[5] The objective was to protect the research and possible applications of nuclear energy.

During World War II the United States developed significant knowledge of nuclear technology that proved extremely valuable to the nation for defensive and offensive purposes. The information gave the United States a significant, critical lead in weaponry that enabled the U.S. to react formidably against Japan's attack at Pearl Harbor, thus turning the tide of World War II in U.S. favor. Indisputably, the United States had a critical need to protect national security by safeguarding nuclear information from improper, unauthorized, or premature disclosure.

Following WWII international developments, later called the Cold War, drove a massive effort within the government to safeguard its secrets from a new adversary, the Soviet Union. Since 1946, the government's secrecy system has been based on a mix of statutes and executive orders, which is an indication of the concern of both the Executive and Legislative branches to control and enforce government secrecy.

ADMINISTRATION OF SECRECY POLICY

Secrecy is administered as a regulatory function of the Executive Branch. The authority to regulate secrecy policy is vested in the President under Article II of the Constitution, which states, "The executive power shall be vested in a President of the United States of America." The Constitution sets forth the general principles out of which the President issues regulatory policy. The legislative and judiciary branches interpret or readapt those principles to the demands of changing times. The Constitution prevents a massive tyrannical government in which all power is vested in one branch. The checks and balances established under our form of government has been successful in maintaining balance between the authority of the

government to establish secrecy policy and the rights and liberties of the citizens to maintain awareness of its government's activities.

The United States Supreme Court, as the independent judiciary advisor to the executive and legislative branches, has affirmed that the President's authority to classify information relating to national security and to prescribe controls on access to such information flows from the Constitution. The President does not need authority granted by congress to classify and keep secret national security information.[6]

EFFORTS TO PROTECT SECRECY

EXECUTIVE ORDERS

With the classification of national security information under the purview of the President, generation and handling procedures are dictated by executive order. As previously mentioned, the development of current day secrecy policy became evident during the World War II era. On March 22, 1940, President Roosevelt issued EO 8381 to protect the development of nuclear weapons from disclosure to adversaries. This policy formalized the government's classification system and specified definitions on what information was subject to secrecy. Three levels of secrecy were established: Secret, Confidential, and Restricted. The policy carried the United States through World War II.

The enactment of the Atomic Energy Act of 1946 separated atomic energy information from strictly related to national security into a separate category. The Act was ratified as legislation rather than executive order because the government considered atomic energy information and its application in nuclear weapons to require more stringent regulation and protection. National security information remained under the control of executive orders.

As the United States was drawn in the Cold War, more restrictive secrecy was needed to ensure the integrity of national military strategy. The increase in secrecy was manifested in President Harry S. Truman signing EO 10104 on February 1, 1950, which limited to the Department of Defense (DoD) the authority to classify information as requiring protection from disclosure. It also added Top Secret as the fourth level of classification.

Administration of secrecy policy was challenging as the need for security spread into such non-defense areas as foreign relations. Non-DoD agencies became involved in actions to enforce government secrecy. Also, as defense agencies engaged in the Korean War, mounds of paperwork were generated. This made the need to manage information and security measures readily apparent. Consequently, on September 24, 1951, President Truman expanded classification authority to non-DoD agencies by signing EO 10290, "Prescribing

Regulations Establishing Minimum Standards for the Classification, Transmission, and Handling, by Departments and Agencies of the Executive Branch, of Official Information Which Requires Safeguarding in the Interest of the Security of the United States." The order enhanced management of secrecy policy by providing downgrading and declassification instructions. It allowed national security information to be eventually decontrolled and released to the public after it had served its purpose and was considered no longer sensitive to the national security strategy.[7]

As the United States continued to build offensive and defensive strategies for the Cold War, trends in policy on government secrecy fluctuated, seemingly as democrats and republicans occupied the White House. Americans were becoming more aware of international activities. The Korean War was brought into the homes of Americans by technological developments in television and increased press coverage. The new awareness fed a desire for more information. Consequently, the public demand for openness in government increased.

President Dwight D. Eisenhower refined administrative handling of classified information striving for a balance between openness and secrecy. On December 15, 1953, he issued EO 10501 to reduce the number of agencies authorized to classifying information and eliminated the Restricted level of protection. As the Soviet Union and the United States battled for international superiority in the Cold War, the enforcement of policy to guard against unauthorized disclosures of national security information became critical. In 1961, President John F. Kennedy amended Eisenhower's secrecy policy by issuing EO 10964. It added a provision that any person who divulged classified information would be subjected to administrative sanctions.

During the Vietnam War era Americans openly exercised their rights to question national security policy on secrecy, especially on military strategy and US involvement in Vietnam. Public pressure reigned through demonstrations publicized internationally. US involvement in the Vietnam War brought strained relations between the American people and the government. Public mistrust of the government increased greatly due to the lack of public understanding of national security policy and the nation's changing participation in military operations in Asia.

Relenting to public and political pressure President Richard Nixon relaxed the requirements of the classification system by issuing EO 11652 on March 8, 1972. The directive reduced further the number of government agencies authorized to classify information and set mandatory provisions for periodic review of classified holdings. These actions were intended to gain public trust while protecting government secrets – for a set duration. Subsequent to the Vietnam War, public mistrust prevailed as a political issue.

The Watergate scandal caused the downfall of Nixon, leaving President Gerald Ford to help the nation recover its confidence in government. In the wake of Watergate the public pushed for greater awareness of government activities with emphasis on truthful information. Soon after taking office President Jimmy Carter brought the greatest attack on government secrecy. He relaxed the tight reigns on secrecy by the issuance of EO 12065 on June 28, 1978. A radical change to the rigid structure of the classification system, this directive allowed broad use of classification authority to be challenged. It required "identifiable damage" for Confidential information rather than simple "damage." This difference was predicated on legal justification to specifically identify or project what damage to the national security would be caused upon disclosure of the information. The order also mandated a balance test of public interest versus possible damage to the national security before the classification of information. President Carter also established a means to watch and manage use of the classification system by creating the Information Security Oversight Office. In all, the policy on secrecy shifted toward more openness in government by less use of the classification system.

President Ronald Reagan reversed the trend toward openness by replacing the Carter policy with a more conservative directive. On April 2, 1982, he issued EO 12356 which overturned the "identifiable damage" requirement for Confidential information. The order allowed moderate use of the protective system especially when doubt existed on whether to classify and when to apply declassification dates. One of the policy's major revisions allowed the unprecedented reclassification of declassified and released national security information under certain conditions. Public attitude did not object to this significant change in secrecy policy.

With the election of President William J. Clinton the U.S. secrecy policy returned to the liberal provisions of the Carter era upon issuance of EO 12958 on April 16, 1995. This directive imposed a new ten-year limit on classification actions. It mandated automatic declassification of information that is over 25 years old. Agencies were required to establish systematic declassification review programs and declassify old records within five years. The directive also returned the balancing test for weighing public interest in disclosure against potential damage to national security.[8] The greatest feature of this policy was the requirement to clean out tons of old classified records relating to the Cold War era.

> Public service is a public trust. The highest obligation of every individual in government is to fulfill that trust. Each person who undertakes the public trust makes two paramount commitments: to serve the public interest and to perform with integrity.
>
> —Elliot Richardson

The Federal government has an elaborate and diversified security program to exercise its secrecy policy. The program is divided into many facets of security, addressing personnel, information, operations, communications, facilities (physical security), contractors (industrial security), technical security countermeasures, and awareness and education. Although each security program or discipline is distinct in technical application, they overlap considerably and are most effective when integrated fully. For example, personnel are approved for access to national security "classified" information under the personnel security program. An information security specialist provides a security briefing, developed as part of the awareness and education program, to educate the newly cleared employee on procedures for handling classified information. Included in the briefing are procedures for physical protection (facilities such as restricted working areas and vaults) and access to contractors covered by the industrial security program. Communications and operations security are special applications of security measures that pertain to unique and technical environments. The integration of all security measures maximize protection of information as it flows through applications, e.g., communicating classified information around the world, from government agency to contractor, or from electronic form to paper copy.

There are three requirements for access to classified national security information. First, a person who is an employee, contractor, licensee, or grantee of the Federal government and occupies a position requiring access to national security information is subjected to a personal background investigation. The investigation is used to establish a level of assurance or trust that the person will protect the information when given access. Once the investigation is completed, it is evaluated for any indications of potential mistrust. If the findings are favorable, the employing agency may grant a security clearance. By itself the security clearance does not allow access -- it is just one of the three requirements for access to national security information.

The second requirement is to sign a "Classified Information Nondisclosure Agreement," Standard Form 312. The agreement is a legally binding contract between the United States

Government and the individual. By signing it the individual agrees never to divulge national security information to any unauthorized person. The agreement serves as the means of informing the signer of responsibilities for protecting national security information and possible penalties of noncompliance. If an individual violates the trust implied by the signed agreement, the government is in a better legal position to apply discipline through civil or administrative action for disclosing national security information. Included in the agreement is an acknowledgement that the signer has received indoctrination on the nature of national security information and protective security procedures.

The third requirement is a valid need to know the information to perform official duties. A determination of the need to know is made by the holder of the national security information. The holder of the information must also confirm the recipient's identity and security clearance level. Once an individual gains access to national security information, he or she will assume responsibility for ascertaining the need to know of any following recipients.

PROMOTING OPENNESS IN GOVERNMENT

> A popular Government without popular information or the means of acquiring it, is but a Prologue to a Farce or a Tragedy or perhaps both. Knowledge will forever govern ignorance, and a people who mean to be their own Governors, must arm themselves with the power knowledge gives.
>
> —James Madison

A government where secrecy prevails is a tyranny. Where citizens have no rights to know the activities of their government, the government ceases to serve its people. The advent of technology over past decades has given Americans access to information never before imagined. Consequently, the thirst for information has grown considerably. The passage of two major laws brought considerable change in government secrecy: the Freedom of Information Act and the Privacy Act.

FREEDOM OF INFORMATION ACT

On July 4, 1966, President Lyndon Baines Johnson grudgingly signed into law the United States Freedom of Information Act (FOIA), marking the first major advancement for openness in government.[9] The Act (5 United States Code, Section 552 or Public Law 89-554) establishes the means for the public to access information created by or in the possession of federal government agencies. Before issuance of the Act the burden to establish a right for access to

government information was on the requester. No statutory or judicial solutions existed to help a person seeking information from the government. The FOIA caused a shift in the burden from the individual to the government. It required government agencies to disclose information to the fullest extent possible. Under the FOIA the government must justify its need for secrecy upon denying information to a requester.

The FOIA does not apply to information produced or held by federal elected officials including the President, Vice President, senators and congressmen. It also allows the government to withhold certain information covered by nine exemptions. The exemptions include:

- national security information that concerns national defense or foreign policy and has been properly classified under executive order;
- information on an agency's internal personnel rules and practices;
- information exempted by other federal statutes;
- trade secrets, commercial or financial information;
- inter-agency or intra-agency communications such as memoranda and letters that would normally not be available by law;
- personal information, when disclosure of the information would be an invasion of a person's privacy;
- law enforcement information, to the extent that the information could interfere with law enforcement events, would deprive someone of a fair trial, would result in an invasion of personal privacy, would identify a confidential source, circumvent the law, or would endanger a person's life or physical safety;
- records on financial institutions; and
- geographical and geophysical information on wells.[10]

An amendment to the FOIA (Public Law 104-231) expanded the law's definition of "record" to include information collected and maintained by an agency regardless of format. This action

was intended as a matter of increasing efficiency in government by encouraging agencies to use technology – electronic file formats, automated indices of releasable records, and web sites.

Agencies of the Federal Government have resisted compliance with the FOIA over the years, especially the mandatory 20 working day turnaround of FOIA requests. For example, the Central Intelligence Agency took nine years to deny an FOIA request for 22 documents. However, documents released by the government under the FOIA have exposed information of great public interest. Examples include disclosures of high mercury levels in canned tuna, disparities in drug prescriptions, and cost overruns of government programs.[11]

PRIVACY ACT

A companion to the Freedom of Information Act is the Privacy Act of 1974. The Privacy Act (Public Law 93-579 or 5 U.S.C. Section 552a) regulates the record keeping and disclosure practices of government agencies, which enables Americans to get access to government records about themselves. It restricts government agencies from disclosing personally identifiable information. Along with the FOIA, the Privacy Act restricts disclosure of personal information when disclosure to others would violate the person's privacy. To prevent government agencies from keeping secret files on individuals, agencies must publicly describe each of its systems of records that contain personal information.

An example that applies to the Privacy Act is government files containing individual electronic mail (e-mail) addresses. When government agencies intentionally collect e-mail addresses for databases or mailing lists the agencies must notify the public that they collect the information and explain why. In this instance the e-mail address is considered personally identifiable information.

Both the FOIA and Privacy Act support disclosure of information and conversely recognize a legitimate need by the government to limit disclosure of some information, such as information relating to criminal investigations, foreign relations, defense issues, or national security. Essentially, both statutes require government agencies to be accountable for policies and procedures on disclosing information. They ensure that a requester of information will receive a response to his or her request. If the information requested cannot be released, the requester must be given the reason for the denial. The requester may appeal the denial to include challenging the denial in court. The FOIA and Privacy Act are valuable tools to ensure that disclosure of government information is not arbitrary and that government actions can be reviewed.[12]

POLICY ON MANAGEMENT OF FEDERAL INFORMATION RESOURCES

The Office of Management and Budget (OMB) is an Executive Branch agency responsible for overseeing the management and allocation of financial and informational resources. OMB issued Circular A-130 to provide federal agencies guidance on implementing the Paperwork Reduction Act (Public Law 104-13 or 44 U.S.C. Section 35). The Act addresses collection of information from the public and information dissemination and access practices within the government. OMB Circular A-130 instructs agencies to be proactive in disseminating information, rather than waiting to respond to a public request for information. It directs agencies to assist the public in gaining access to government information through a mixture of electronic and other means.

OVERSIGHT OF THE SECRECY SYSTEM

The government has established internal organizations to oversee the security classification system and to regulate secrecy policy. The Information Security Oversight Office and the Security Policy Board are within the Executive Branch. The Congress (103rd session) established the Commission on Protecting and Reducing Government Secrecy.

INFORMATION SECURITY OVERSIGHT OFFICE

The Information Security Oversight Office (ISOO) was created in 1978 to oversee the classification, declassification and protection of national security information. It is placed organizationally as an administrative component of the National Archives and Records Administration but receives its policy and program guidance from the National Security Council. ISOO is responsible to the President for policy oversight of programs for safeguarding national security information in government and industry. It has purview over 60 executive branch agencies that generate and/or handle national security information.

ISOO reports annually to the President on the status of the security classification system. It provides statistics and analysis on the system as trend indicators of classification activity. This activity demonstrates swings in the balance of secrecy and openness in government. ISOO uses the trend indicators to enhance national secrecy policy and internal government guidance on the security classification program.

In its 2001 Report to the President, ISOO reported that an upward trend in classification activity continued from past years. With the ongoing global war on terrorism little change was expected for the next year. ISOO also reported that the executive branch continued to declassify old permanent records, which have great value to recording the nation's history.

During 2001 government agencies declassified and released 100,104,990 pages of historical records.[13]

SECURITY POLICY BOARD

As the United States experienced the end of the Cold War the government needed to manage more closely its national policy on secrecy. The economic status of the country began to compete with resources previously demanded by national security and political issues. A Joint Security Commission of the Director of Central Intelligence and the Secretary of Defense recommended to President Clinton a revision to national security policy. The revision focused on the need to analyze threats to the nation and manage risks. On September 16, 1994, President Clinton issued Presidential Decision Directive/NSC – 29 (NSDD/NSC 29).

NSDD/NSC 29 established the Security Policy Board -- a new security policy structure under the purview of the National Security Council – to "… consider, coordinate, and recommend for implementation to the President, through the Assistant to the President for National Security Affairs, policy directives for U.S. security policies, procedures and practices." It offered four principles to guide formulation, evaluation, and oversight of the nation's security policy.

- Ensure security policies and practices are realistic in matching threats and flexible to adjust as threats change.
- Ensure security policies and practices are consistent and effective in managing resources.
- Ensure security standards and procedures are fair and equitable in their treatment of U. S. citizens.
- Ensure security policies, practices and procedures provide security that is necessary and affordable.

Member agencies of the Security Policy Board included the Director of Central Intelligence, the Deputy Secretary of Defense, Vice Chairman of the Joint Chiefs of Staff, the Deputy Secretary of State, the Under Secretary of Energy, the Deputy Secretary of commerce,

the Deputy Attorney General, one Deputy Secretary from a non-defense agency, and a representative from the Office of Management and Budget and the National Security Council. This representation brought together defense and civilian agencies of the Executive Branch – producers and users of classified national security information.

NSDD/NSC 29 also created a Security Policy Advisory Board to serve as a private (non-governmental) body to advise the President from a public interest perspective on national security policy issues. The members of this board were appointed by the President, which could allude to questionable political influence of a public interest perspective. [14]

Four years after the Security Policy Board was established questions arose as to whether it was effective in performing its mission. The intent of the Board was to create security standards and practices across government that were sensible and cost-effective. Since its conception, the Board has made little progress toward minimizing redundancies and complexities of the government's system of maintaining secrecy of information.[15]

As an interagency entity, the Security Policy Board – with a membership of 35 federal agencies – had its problems. Agencies that are not in full agreement with a proposal could delay or dilute an action, thus undermining the intent in creating the Board. Another factor was the infrequency of formal meetings. Other business of the primary representative agencies tended to override the mission of the Board; consequently, members communicate by telephone and computer. Failing to meet personally – face to face – allowed significant issues to be ignored or delegated to subordinates. It also suggested that the Board had no reason to meet, which reflected upon the government that revising or enhancing security standards and practices was not a high priority for the administration.

CONGRESSIONAL OVERSIGHT

A recent effort in congressional monitoring of national secrecy policy was through the Commission on Protecting and Reducing Government Secrecy. The Commission was created during the 103rd Congress (1997) to explore ways to control government secrecy while ensuring protection for the information that truly required it. Through this effort, the congress reexamined secrecy and openness to explore new ways of thinking about government secrecy.

The congressional report stated that two security disciplines stand out as being particularly unsuccessful in protecting information most critical to national security: personnel security and information security, as the latter applies to the security classification system for national security information. Many people inside and outside of government no longer trust these two disciplines. The report stated, "Even as billions of dollars are spent each year on

government secrecy, the classification and personnel security systems have not always succeed at their core task of protecting those secrets most critical to the national security. The classification system, for example, is used too often to deny the public an understanding of the policymaking process, rather than for the necessary protection of intelligence activities and other highly sensitive matters."[16]

The report also stated, "Some two million Federal officials, civil and military, and another one million persons in industry, have the ability classify information. Categories of administrative markings also have proliferated over time, and the secrecy system has become ever more complex." The implication is that the government's security system is broke, that too many government officials have the authority to impose security restrictions on some government information and that there are too many varieties of security measures for safeguarding such information.[17]

CURRENT NATIONAL SECRECY POLICY

Today, the government's secrecy policy continues to be embodied in national security information protected from disclosure pursuant to Executive Order (EO) 12958, "Classified National Security Information." President Clinton issued the directive on April 17, 1995. Two subsequent presidential directives, Executive Orders 12972 and 13142, have amended EO 12958 to clarify definitions and extend certain deadlines imposed by EO 12958.

Clinton's executive order represented a departure from the secrecy policies of the past. It revised the security classification system for the first time since the end of the Cold War. It caused a sharp increase in openness in government by instituting requirements to declassify old permanent records. The declassification provisions of the order were major reforms in the security classification system by requiring historically valuable records to be automatically declassified as they became 25 years old. Executive orders of the past allowed classified records to remain classified indefinitely.

EO 12958 remains as the prevailing national secrecy policy by the Bush administration. Changes to the policy are under consideration but they primarily address administrative procedures, such as extensions of deadlines imposed to dispose of the multitude of old classified records. Activity within the Bush administration has been to move the trend toward an increase in government secrecy. However, this is seen in numerous internal government memoranda; no executive order has been issued to withdraw EO 12958.

Though the administration continues to apply EO 12958, President George W. Bush established the means of reviewing the order by signing National Security Presidential Directive

(NSPD) 1 on February 13, 2001. NSPD 1 creates several Policy Coordination Committees, under the purview of the National Security Council, to coordinate national security policy in an interagency forum.[18]

The chair of the Policy Coordination Committee for Records Access and Information Security, established under NSPD 1, however, created the Classification Management Working Group to explore any need to revise EO 12958. Several changes to EO 12958 are under consideration. Most of the proposed changes apply to section 3.4, "Automatic Declassification." Work on the changes is anticipated to continue for a year or more.[19]

The increase in global terrorism was instrumental in forcing slight changes in national secrecy policy by the Bush administration. Terrorist attacks on the USS Cole, the New York Trade Center buildings and the Pentagon, and a downed plane in rural Pennsylvania were stark reminders of the growing threat to Americans. Additionally, impending war with Iraq focused a need to ensure protection and integrity of military strategy and political negotiations with foreign allies, as well as other potentially sensitive information. Although the Bush administration did not move forward to issue any executive order to change EO 12958, a focus on national security policy brought a significant increase in government secrecy.

In the early stages of building Bush's secrecy policy, Andrew Card, Assistant to the President and Chief of Staff, issued a memorandum to heads of executive departments and agencies. It reminded agency heads of their obligation to safeguard records on weapons of mass destruction (WMD) on an ongoing basis and upon receipt of a request for such information under the Freedom of Information Act. It disseminated guidance to review holdings of information on weapons of mass destruction and information that could be misused to damage national security and public safety. The memorandum guided agencies to continue classification of national security information beyond its 25-year expiration date and allowed classification or reclassification of unreleased information on WMD. Furthermore, it cited the need to protect from inappropriate disclosure any potentially sensitive information that failed to meet the standards for classification.[20]

Within the Department of Defense notices were distributed to all personnel as a strong reminder of the obvious. Namely, a memorandum issued jointly by the Secretary of the Army and Army Chief of Staff states, "The unauthorized intentional release of classified information is absolutely unacceptable and is punishable by law. At best, such leaks compromise the options of our policymakers at the national level. At worst, they kill people." It serves as a keen reminder that detailed knowledge of military strategy and plans is vital to national security and mission success, and must be properly protected. Conversely, the memorandum was soft on

conveying the American public's constitutional right to know the activities of its government. It deferred to political officials the responsibility to resolve the "healthy tension" between the American people and their government on knowledge of military activities. If the Army's memorandum is indicative of the Bush administration's position on government secrecy, it might imply the attitude of "us versus them" and that all Army personnel are not employed to serve the American public. [21]

U.S. secrecy policy is viewed differently outside the country. At the 2001 Annual Symposium of the American Society of Access Professionals, a representative from France challenged the presenter from the United States. The Frenchman asked why the U.S. would boast of significant advances in declassifying old records as it would only bring criticism from openness proponents in the U.S. and more criticism from abroad. He claimed that foreign governments feel threatened by the U.S. practice of declassifying and releasing records. In France, he claimed, the government does not declassify records. None of its citizens complain and damaging disclosures would hurt none. Ironically, some weeks following that exchange the U.S. presenter met with a former French army general who had served several years in Washington, D.C., as a military liaison. The general indicated that he was assigned to develop a system for declassification of French military records and he wished to find out how the U.S. declassification system worked. He later mentioned his amazement of the level of openness in the U.S. government and considered it the best feature of our government.[22]

As the United States prepares for war in the Middle East many countries are looking to the U.S. to share its intelligence information as to the growing threats to their citizens and commercial industries. One particular threat is to commercial transportation systems used to move U.S. military forces. General John Handy, U.S. Transportation Command, as reported by the New York Times, said that a password-protected website was being established to share "sanitized" intelligence information with private freight and passenger transportation companies. How quickly and effectively this can be carried out concerns some government officials who are worried about dissemination restrictions placed on information by its originating government agency. [23]

Pressures placed on the U.S. secrecy policy causes one to wonder how well the government's secrecy system is working. Effectiveness of secrecy policy and the security classification system can be measured by an agency's profile on secrecy and openness. For example, government agencies employ professional staffs to carry out statutory and regulatory provisions in managing secrecy. The attitudes of these staffs affect the agency's profile much more than adherence to policy or law. The former director of ISOO reported that agencies like

the Departments of Defense and State were seldom involved in litigation of FOIA requests, unlike the Departments of Treasury and Agriculture that were constantly defending their actions in court. The reasons cited were attorneys and information officers of some agencies believe in the public's right to know the activities of government, unless national security interests prevailed. These professional staffs would coordinate closely with FOIA requesters and usually resolve issues amicably. The staffs of other agencies believed just as much that it was their duty to withhold as much information as possible from the public. FOIA requesters were viewed as the enemy and coordination, if done at all, was always adversarial. Within a few years of FOIA being enacted, staffs had established for their agency a distinct FOIA profile – either for or against openness in government.[24]

Another indicator of the effectiveness of secrecy policy is how quickly information that no longer requires protection is moved out of the security system, or is not classified in the first place. In today's society Americans have multitudes of information available via the Internet. Government information, unfortunately, is absorbed by the security system too often, as if the information revolution never occurred.

CONCLUSION

Since security policy is carried out by Executive Order, the President has the latitude to amend or change the policy as desired, without congressional legislation. This authority provides the Bush administration flexibility to modify secrecy policy so as to influence his policy on foreign relations, American economy, and military strategy. But, has the administration gone too far with its secrecy policy?

Information has no usefulness unless or until it is shared and applied. Information has little value when it is kept secret from the individuals who need it. However, when information is communicated or disseminated its integrity and timeliness become vulnerable and opportunities arise for adversaries to gain access to it. Americans have the inherent right and need to know information about the activities of their government; the government is responsible for ensuring a safe and secure nation for its citizens. The balance is critical in satisfying the citizens' need and right to know information while precluding access to certain information from the nation's adversaries. The open society of the United States demands close attention to maintaining a healthy balance by the people and the government.

In order to have a successful security classification program and credible protective measures the government must also have a reliable declassification program. The American public can put trust and confidence in the government secrecy policy when information that has

served its purpose is declassified and released. For the first time in recent history, Americans are in fear of attacks on their homeland, disrupting their sense of security and safety. Of course, they rely on the government to exercise prudent and swift action to protect the homeland. The desire to feel safe and secure drives the need for increased knowledge of the government's activities.

Public understanding of government policies and actions relies on greater openness. Also, the government can respond to public criticism and justify its actions through greater openness. Openness allows free exchange of scientific, financial, and other socially significant information possible and encourages research and discovery that promote national growth. Openness in government helps young people learn of past actions and prepare for future decisions.

The former head of the Information Security Oversight Office, Mr. Steven Garfinkel, stated that "…the American government stands apart, far apart, from any other government, either now or in the past, in the quality and quantity of information it shares with its citizens and the world. This openness is a defining statement about the kind of democracy we are. It is a defining statement about America."[25]

Where are we today with secrecy in government? Mr. J. William Leonard, newly appointed Director, Information Security Oversight Office, stated in a recent address, "the issue is not one of openness vs. secrecy. One could not be had without the other." He indicated further, "What makes our Nation great is not how well we can make and keep secrets. Rather it is our legacy of an open government – a defining factor of our democracy."[26]

A simple understanding is the American public will support the government when it feels well informed of government activities. The public has historically given its support and trust when government leaders are true and honest in their communications to the nation. The government should not sell the public short on the ability to understand that certain information – national security information and other sensitive information – cannot be disclosed publicly. It is incumbent on the government to use its secrecy policy responsibly and prudently and communicate with its citizenry in a fashion that is appropriate for ensuring positive and healthy economy, defense, and social structures. Under the Bush administration the balance between secrecy and openness is leaning in favor of secrecy, and for good reason. The security of a nation at war demands it.

WORD COUNT = 6,917

ENDNOTES

[1] William J. Clinton, "Classified National Security Information," Executive Order 12958, (Washington, D.C.: The White House, 17 April 1995) 1.

[2] Congress, Senate, Report of the Commission on Protecting and Reducing Government Secrecy, 103rd Congress, 1997, xxi.

[3] Sun Tzu, The Art of War, quoted by N. Cathy Maus, U.S. Department of Energy, History of Classification and Declassification, (Washington, D.C.: 22 July 1996) 1.

[4] N. Cathy Maus, History of Classification and Declassification, Department of Energy, (Washington, D.C.: 22 July 1996) 2.

[5] Ibid., 1.

[6] George W. Bush, "Defense Bill Signing Statement," Press Release, (Washington, D.C.: The White House, 10 January 2002) 2.

[7] Maus, 5.

[8] "U.S. Government Information: Executive Orders Declassifying Information," Yale University Library, Government Documents and Information Center, 23 April 2002, available from <http://www.library.yale.edu/govdocs/declord.html>; Internet; accessed 8 September 2002.

[9] "The FOIA and President Lyndon Johnson," The National Security Archive [journal on-line]; available from http://www.gwu.edu/~nsarchiv/nsa/foia/lbj.html; Internet; accessed 8 September 2002.

[10] Freedom of Information Act, U.S. Code, volume 5, section 552(b) (4 July 1966).

[11] "The U.S. Freedom of Information Act at 35: Nearly 2 Million Requests Last Year at a Cost of One Dollar Per Citizen," The National Security Archive [journal on-line]; available from http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB51/; Internet; accessed 8 September 2002.

[12] "A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records," available from <http://www.tncrimlaw.com/foia/II.thml>; Internet, accessed 27 January 2003.

[13] J. William Leonard, letter on Information Security Oversight Office's 2001 Report to the President, Washington, D.C., 20 September 2002.

[14] William J. Clinton, "Security Policy Coordination," Presidential Decision Directive/NSC 29, (Washington, D.C.: The White House, 16 September 1994), 3.

[15] Ibid.

[16] Congress, xxi.

[17] Ibid, xxvi.

[18] George W. Bush, “Organization of the National Security Council System,” memorandum for the Vice President and others, Washington, D.C., 13 February 2001.

[19] Paul Laplante, “Revision of Executive Order 12958,” ONNSI Communique, Department of Energy. Washington, D.C., August 2001.

[20] Andrew H. Card, Jr., “Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security,” memorandum for the Heads of Executive Departments and Agencies, Washington, D.C., 19 March 2002.

[21] Eric K. Shinseki and Thomas E. White, “Army Directive #4 – Handling Classified Information,” memorandum for All Army Personnel, Washington, D.C., 2 August 2002.

[22] Steven Garfinkel, “Presentation of Steven Garfinkel, Director, Information Security Oversight Office, Before the American Society of Access Professionals,” 11 December 2001.

[23] Thomas Shanker, “Officials Reveal Threat to Troops Deploying to Gulf.” New York Times, 13 January 2003.

[24] Garfinkel.

[25] Ibid.

[26] Leonard, J. William, Director, Information Security Oversight Office. Remarks at the National Classification Management Society Annual Training Seminar. Fort Worth, Texas. July 16, 2002.

BIBLIOGRAPHY

Aldridge, E.C. "Pete", Jr., Under Secretary of Defense (AT&L). Letter to Industry Partners. Washington, D.C., 2 October 2001.

Ashcroft, John, Attorney General. Letter to Congress and The President. Washington, D.C., 22 October 2002.

Bush, George W., President. "Congressional Subpoena for Executive Branch Documents." Memorandum for the Attorney General. Washington, D.C., 12 December 2001.

_____. "Defense Bill Signing Statement." Press release. Washington, D.C., 10 January 2002.

_____. "Disclosures to the Congress." Memorandum to Secretaries of State, The Treasury, and Defense, Attorney General, Director of Central Intelligence, and Director of Federal Bureau of Investigation. Washington, D.C., 5 October 2001.

_____. "Organization of the National Security Council System." National Security Presidential Directive 1. Washington, D.C., 13 February 2001.

_____. "Organization of the National Security Council System." Memorandum for the Vice President and others. Washington, D.C., 13 February 2001.

_____. "Statement by the President on H.R. 2883, the Intelligence Authorization Act for Fiscal Year 2002." Press release. Washington, D.C., 28 December 2001.

Card, Andrew H., Jr., Assistant to the President and Chief of Staff. "Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security." Memorandum for the Heads of Executive Departments and Agencies. Washington, D.C., 19 March 2002.

Clinton, William J., President. Executive Order 12958, "Classified National Security Information." Washington, D.C., 17 April 1995.

_____. Executive Order 12972, "Amendment to Executive Order No. 12958." Washington, D.C., 18 September 1995.

_____. Presidential Decision Directive/NSC 29. "Security Policy Coordination." Washington, D.C., 16 September 1994.

Clymer, Adam, New York Times News Service. "Bush Sets New Secrecy Standard – Sept. 11 one reason behind clampdown." The Sun Herald. 3 January 2003.

Congress. U.S. House of Representatives. Congressional Record. "Testimony on Senate Bill 1160. Washington, D.C., 20 June 1966.

Congress. U.S. Senate. Report of the Commission on Protecting and Reducing Government Secrecy. Washington, D.C., 1997.

Department of Homeland Security. "Classified National Security Information." Federal Register, Rules and Regulations, Volume 68, Number 17. Washington, D.C.

Fleischer, Ari, Press Secretary, The White House. "Transcript: Press Briefing by Ari Fleischer." Washington, D.C.: 24 September 2001.

Freedom of Information Act. United States Code, Volume 5, Section 552(b). Washington, D.C.: 4 July 1966.

Garfinkel, Steven, Director, Information Security Oversight Office. "Information Security Oversight Office 2000 Annual Report." Letter to the President. Washington, D.C.: 17 September 2001.

_____. Presentation Before the American Society of Access Professionals 2001 Annual Symposium. 11 December 2001.

Holman, Kwame. "Spies Among Us." 9 June 1999. Online NewsHour. Available from <http://wwwpbs.org>. Internet. Accessed 28 February 2003.

Information Security Oversight Office. Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet. Washington, D.C.: 1985.

Information Security Oversight Office. "Statement of Impact of Executive Order 13142, Amendment to Executive Order 12958." Washington, D.C.: 19 November 1999.

Laplante, Paul. Office of Nuclear and National Security Information, U.S. Department of Energy. "Revision of Executive Order 12958." Washington, D.C.: August 2001.

Lardner, Richard. "Keeping Secrets." Government Executive Magazine. Washington, D.C.: 1 March 1998.

Leonard, J. William, Director, Information Security Oversight Office. "Information Security Oversight Office 2001 Annual Report." Letter to the President. Washington, D.C.: 20 September 2002.

_____. "Remarks at the National Classification Management Society Annual Training Seminar." Fort Worth, Texas: 16 July 2002.

Maus, N. Cathy. U.S. Department of Energy. "History of Classification and Declassification." Washington, D.C.: 22 July 1996.

Priest, Dana, Washington Post Staff Writer. The Washington Post. Telling Secrets: Not Just What, but How – Speech is Revealing on Gathering Intelligence. Washington, D.C.: February 6, 2003.

Project on Government Secrecy, Federation of American Scientists. Bush Administration Documents on Secrecy Policy. Washington, D.C.: 2003.

Project on Government Secrecy, Federation of American Scientists. Information Security Oversight Office. Washington, D.C.: 2003.

Rumsfeld, Donald, Secretary of Defense. The Impact of Leaking Classified Information. Washington, D.C.: 12 July 2002.

Schroeder, Gerald A. U.S. Department of Justice. FOIA Update, Volume III, Number 3, An Overview of Executive Order 12356. Guest Article. Washington, D.C.: June 1982.

Security Policy Advisory Board. Annual Report – CY 2000. Washington, D.C.: 25 January 2001.

Shanker, Thomas, New York Times. Officials Reveal Threat to Troops Deploying to Gulf. New York City, New York: 13 January 2003.

Shinseki, Eric K., General, U. S. Army, Chief of Staff, and White, Thomas E., Secretary of the Army. Army Directive #4 – Handling Classified Information. Memorandum for All Army Personnel. Washington, D.C.: 2 August 2002.

The National Security Archive. "The U.S. Freedom of Information Act at 35: Nearly 2 Million Requests Last Year at a Cost of One Dollar Per Citizen." Available from <http://www.gwu.edu>. Internet. Accessed 8 September 2002.

TNCRIMLAW Website. "A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records." Available from <http://www.tncrimlaw.com>. Internet. Accessed 27 January 2003.

Tzu, Sun. The Art of War. Quoted by Maus, N. Cathy, U.S. Department of Energy. "History of Classification and Declassification." Washington, D.C.: 22 July 1996.

U. S. Department of Energy, Office of Nuclear and National Security Information. "Revision of Executive Order (E.O.) 12958." Washington, D.C.: August 2001.

U. S. Department of Justice. "New Attorney General FOIA Memorandum Issued." Washington, D.C.: 2003

U.S. Department of Justice. FOIA Update, Volume VI, Number 1. "Protecting National Security Under the FOIA." Washington, D.C.: Winter 1985.

U.S. Department of Justice. FOIA Update, Volume XVI, Number 2. "FOIA Focus: Steve Garfinkel." Washington, D.C.: Spring/Summer 1995.

_____. "New Executive Order on Classification of National Security Information Issued."

Washingtonpost.com. "Recent Major U.S. Espionage Cases." Washington, D.C.: 8 March 2001.

White House. "H.R. 4598 – Homeland Security Information Sharing Act." Statement of Administration Policy. Washington, D.C.: 26 June 2002.

Yale University Library, Government Documents and Information Center. "U.S. Government Information: Executive Orders Declassifying Information." Available from <http://www.library.yale.edu/govdocs/declord.html>. Internet. Accessed 8 September 2002.